

التوقيع الإلكتروني المتقدم (AES): ورقة الامتثال

مستوى التوقيع والاحتفاظ بالأدلة والاستضافة

آخر تحديث: 12 أكتوبر 2026

مستوى التوقيع

توقيع إلكتروني متقدم بالمعنى الوارد في المادة 26 من اللائحة (الاتحاد الأوروبي) رقم 910/2014 (eIDAS). ويستند إلى المتطلبات الأربعة التالية.

- 1 مرتبط بالموقع بشكل فريد: يُنشأ زوج مفاتيح شخصي في متصفح الموقع ويُصدر شهادة خاصة بهذا التوقيع.
- 2 التحقق من هوية الموقع: رابط توقيع شخصي يُرسل بالبريد الإلكتروني، ثم رمز لمرة واحدة يُرسل برسالة نصية إلى هاتفه المحمول. قناتان منفصلتان.
- 3 تحت السيطرة الحصرية للموقع: المفتاح الخاص غير قابل للتصدير ولا يغادر متصفحه أبداً.
- 4 أي تعديل لاحق يمكن اكتشافه: محتوى المستند مختوم ببصمة SHA-256 وموقعة وبختم زمني RFC 3161.

الأدلة المسلمة

يرافق كل مستند موقع شهادة إثبات: أحداث مختومة زمنياً (الفتح، استلام الرمز، التوقيع)، وعنوان IP، ورقم الشهادة، وبصمة المستند.

الاحتفاظ

تُحفظ المستندات الموقعة وسجلات التدقيق لمدة 10 سنوات، أيّاً كان الاشتراك المختار.
لا تُحذف بعد 30 يوماً إلا البيانات المنشأة بمفتاح اختبار (بيئة التجربة).

الاستضافة وحماية البيانات

يعمل التطبيق وقاعدة البيانات وتخزين المستندات على بنيتنا التحتية الخاصة داخل الاتحاد الأوروبي (مزود الاستضافة IONOS). تشفير TLS 1.3 أثناء النقل و AES-256 أثناء التخزين. يمكن توقيع اتفاقية معالجة البيانات (DPA) وفق اللائحة العامة لحماية البيانات عبر الإنترنت من حساب العميل.

للعلم

يُقدّم التوقيع المؤهل (QES) لكل توقيع عبر مزود خدمات ثقة مؤهل شريك؛ وتصف هذه الورقة المستوى المتقدم فقط. شهادة ISO 27001: تدقيق الاعتماد جارٍ ولم تُمنح الشهادة بعد.